UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/563,258	01/04/2006	Takeshi Iwatsu	277188US6PCT	9948

22850 7590 08/26/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
HOANG, SON T	
ART UNIT	**PAPER NUMBER**
2165	

NOTIFICATION DATE	DELIVERY MODE
08/26/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/563,258	IWATSU ET AL.	
	Examiner	Art Unit	
	SON T. HOANG	2165	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10-17 and 19-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-17 and 19-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *17 July 2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 11, 2008 has been entered.

Response to Amendment

2. **Claims 1**, **10**, **19**, and **24** have been amended.

Claims 1-8, **10-17**, and **19-31** are pending in this instant Office action.

Response to Arguments

3. Applicant's sole argument towards **claims 1**, **10**, **19**, and **24** regarding the fact that Yuji does not teach or disclose the deletable data attribute is based on whether or not the data was copied from external storage medium.

The Examiner concurs to the above remark. However, it is noted that Schran et al. (*Pub. No. US 2002/0143770, filed on March 28, 2001; hereinafter Schran*). anticipates the argued limitation. Accordingly, Schran teaches the privacy scanning algorithm to remove unwanted cookie files from the client machine 20. The privacy scanning algorithm determines which cookie files are to be removed (scrubbed) from the client machine 20 by analyzing the privacy protection criteria residing within the local copy of the watch list 14, the trustlist 16 and the blacklist 18. As depicted in the table

shown in Figure 5, if a cookie file is listed on the watch list, but not on the trustlist, the cookie file will be scrubbed or blocked. Any time that a cookie file appears on the blacklist, the cookie file will be scrubbed or blocked regardless of whether or not it appears on the watch list. The Privacy Scanning Algorithm may be carried out in a periodic mode wherein the algorithm is executed at a regular interval, specified by the user, to detect and remove unwanted cookie files from the client machine ([0033]). See further Figure 6 for example of blacklisted websites. Note that by definition, a website is a collection of web pages, images, video or other digital assets that is hosted on one or more web servers (e.g. a computer).

It would have been obvious to an ordinary person skilled in the art at the time of the invention was made to incorporate the teachings of Schran with the teachings of Yuji for the purpose of allowing a user to screen cookie files to determine which cookie files should be stored in the user's client machine (e.g., computer) based on the professional recommendations of a service provider ([Abstract] of Schran).

In view of the above, the Examiner contends that all limitations as recited in the claims have been addressed in this instant Office action. Hence, Applicant's arguments do not distinguish over the claimed invention over the prior arts of record.

Information Disclosure Statement

4. As required by **M.P.E.P. 609(C)**, the Applicant's submission of the Information Disclosure Statement dated July 17, 2008 is acknowledged by the Examiner and all cited documents have been considered. As required by **M.P.E.P 609 C(2)**, a copy of the PTOL-1449 initialed and dated by the Examiner is attached to the instant Office action.

Specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o).

Evidently, the specification fails to provide an explicit definition and/or explanation for the cited "*computer readable medium*" in **claims 19-23**, thus insufficiently supports the claimed medium. Event though the specification defines memory sticks and CDs as examples of computer storage media ([Specification, Page 10]), no examples for computer readable media could be found. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claims 1-8**, **10-17**, and **19-31** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding **independent claims 1**, **10**, **19**, and **24**, Applicant cites two conditional statements. The first one is "*when attribution of said data shows that said data is content copied from an external storage medium*". Only then, the determination of "*the deletion-target priority of said data is high to delete said data*" would be carried out. The claim language clearly shows that when or if attribution of said data does not show that said data was copied from an external storage medium, the process would implicitly do nothing.

The second conditional statement is "*if said determination means determines that the storage of said data is to be performed and a storage medium for storing said data runes out of space*". Only then, the "*deleting data having higher deletion-target priority than others from among a plurality of stored data*" step would be carried out. The claim language clearly shows that when or if storage of said data is not to be performed and a storage medium for storing said data does not run out of space, the process would implicitly do nothing.

Note that changing from '*if*' to '*when*' does not cure the deficiencies of conditional statements. Applicant is suggested to provide an explicit alternate way when a conditional statement is not true. For example, the first conditional statement in **claim 1** "*said control means determining that said deletion-target priority of said data is high to delete said data when attribution of said data shows that said data is content copied from an external storage medium*" needs to provide an alternate solution when it is determined that content is not copied from an external storage medium. One alternate solution could be "*said control means determining that said deletion-target priority of said data is low to delete said data when attribution of said data shows that said data is not content copied from an external storage medium*".

Independent claims 10, **19**, and **24** contain the identical conditional statements as in **claim 1** and must be corrected as explained above.

Each of the **dependent claims 4-8**, **13-17**, **22-23**, and **27-31** contains at least one conditional statement with no alternate solution when the condition is not true / met. They are required to be corrected as suggested in **claim 1**.

Independent claim 19 is further rejected due to having two portions contain repeated subject matters. First portion is from lines 5-8 and second portion is from lines 13-17.

Independent claim 24 is further rejected due to having two portions contain repeated subject matters. First portion is from lines 3-6 and second portion is from lines 13-16.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. **Claims 19-23** are rejected under 35 U.S.C. 101 as being directed to non-statutory subject matters.

Regarding **claim 19**, "*a computer readable medium including computer executable instructions...*" is being recited. Event though the specification defines memory sticks and CDs as examples of computer storage media ([Specification, Page 10]), no examples for computer readable media could be found. Applicant is noted that computer readable media can include storage media (e.g. computer memory, CDs, DVDs, hard drives) as well as propagation / transmission media (e.g. electromagnetic waves, carrier waves, vacuum). By not limiting the claimed "*computer readable medium*" to storage media, Applicant implicitly claimed propagation / transmission media as his invention. As such, the claims are drawn to a form of energy. Energy is not one of the four categories of invention and therefore this claim is not statutory. Energy is not a series of steps or acts and thus is not a process. Energy is not a physical or object

and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a composition of matter.

Claims 20-23 fail to resolve the deficiencies of **claim 19** since they only further limit the scope of **claim 19**. Therefore, **claims 20-23** are also rejected under 35 U.S.C. 101.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. **Claims 1-6**, **10-15**, **19-22**, and **24-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over by Yuji (*Pub. No. JP 2003-173278, published on June 20, 2003*) in view of Schran et al. (*Pub. No. US 2002/0143770, filed on March 28, 2001; hereinafter Schran*).

Regarding **claim 1**, Yuji clearly shows and discloses a data storage control apparatus ([0018]-[0022]), comprising:

data attribution detection means for detecting attribution of storing-target data (*The data is passed to the filer section. Out of the passed data, the filer section identifies expiration date information, significance information and classification information*, [0022]);

determination means for determining whether or not the storage of said data is to be performed based on the attribution of said data detected by said data attribution detection means (*When having passed over the expiration date, (Y) cancels received data (it does not record) and is completed*, [0022]);

data deletion means for deleting data having higher deletion-target priority than others from among a plurality of stored data, if said determination means determines that the storage of said data is to be performed and a storage medium for storing said data runs out of space (*The record control section records the information received from the filter section on a recording device. Here, when the capacity of a recording device is full, the data considered to be the most unnecessary are eliminated in order, judging from significance, classification, information, an expiration date … Moreover, the record*

control section eliminates automatically the information which has passed over the expiration date in the recorded information, [0019]); and

data storage means for storing said storing-target data in said storage medium after said data deletion means deletes data having higher said deletion-target priority (*When the capacity of a recording device is full, the data considered to be the most unnecessary are eliminated in order, judging from significance, classification information, an expiration date, etc., and the information received newly is recorded*, [0019]).

Yuji does not teach the deletable data attribute is based on whether or not the data was copied from external storage medium.

Schran discloses the privacy scanning algorithm to remove unwanted cookie files from the client machine 20. The privacy scanning algorithm determines which cookie files are to be removed (scrubbed) from the client machine 20 by analyzing the privacy protection criteria residing within the local copy of the watch list 14, the trustlist 16 and the blacklist 18. As depicted in the table shown in Figure 5, if a cookie file is listed on the watch list, but not on the trustlist, the cookie file will be scrubbed or blocked. Any time that a cookie file appears on the blacklist, the cookie file will be scrubbed or blocked regardless of whether or not it appears on the watch list. The Privacy Scanning Algorithm may be carried out in a periodic mode wherein the algorithm is executed at a regular interval, specified by the user, to detect and remove unwanted cookie files from the client machine ([0033]). See further Figure 6 for example of blacklisted websites.

Note that by definition, a website is a collection of web pages, images, video or other digital assets that is hosted on one or more web servers (e.g. a computer).

It would have been obvious to an ordinary person skilled in the art at the time of the invention was made to incorporate the teachings of Schran with the teachings of Yuji for the purpose of allowing a user to screen cookie files to determine which cookie files should be stored in the user's client machine (e.g., computer) based on the professional recommendations of a service provider ([Abstract] of Schran).

Regarding **claim 2**, Yuji further discloses said data attribution detection means detects attribution of said data based on applications which request the storage of said data (*A sending set transmits the data of a gestalt which the inverter changed and which can be distributed with a broadcasting mold*, [0018]).

Regarding **claim 3**, Yuji further discloses said data attribution detection means extracts data attribution information which said data contains to detect attribution of said data (*The data is passed to the filer section. Out of the passed data, the filer section identifies expiration date information, significance information and classification information*, [0022]).

Regarding **claims 4**, and **6**, Yuji further discloses the determination means determines the storage of said data is to be performed, if attribution of said data shows that said data is information relating to broadcast contents or said data is broadcast content data (*When it is judged that earthquake information, a heavy rain warning, etc. are important for a user as for the classification information which shows the classification of the contents whose information the and it will change into the data of a*

gestalt which can be distributed, [0018]. *Since the information which can judge when informational important point or needlessness data are received, hence, does not record unnecessary information*, [0029]).

Regarding **claim 5**, Yuji further discloses the determination means determines the storage of said data is to be performed, if attribution of said data shows that said data is now-on-air information including title information of broadcast contents (*Classification information of the important information, i.e., earthquake information, a heavy rain warning etc. may be added with the category information which subdivided an informational classification further*, [0018]. *It is inherent that classification and/or category information contains title of the important news / information*).

Regarding **claim 10**, Yuji clearly shows and discloses a data storage control method ([0018]-[0022]), comprising the steps of:

detecting attribution of storing-target data (*The data is passed to the filer section. Out of the passed data, the filer section identifies expiration date information, significance information and classification information*, [0022]);

determining whether or not the storage of said data is to be performed based on the attribution of said data detected by said detecting (*When having passed over the expiration date, (Y) cancels received data (it does not record) and is completed*, [0022]);

deleting data having higher deletion-target priority than others from among a plurality of stored data, if said determination step determines that the storage of said data is to be performed and a storage medium for storing said data runs out of space

(*The record control section records the information received from the filter section on a recording device. Here, when the capacity of a recording device is full, the data considered to be the most unnecessary are eliminated in order, judging from significance, classification, information, an expiration date … Moreover, the record control section eliminates automatically the information which has passed over the expiration date in the recorded information*, [0019]); and

storing said storing-target data in said storage medium after said data deletion step deletes data having higher said deletion-target priority (*When the capacity of a recording device is full, the data considered to be the most unnecessary are eliminated in order, judging from significance, classification information, an expiration date, etc., and the information received newly is recorded*, [0019]).

Yuji does not teach the deletable data attribute is based on whether or not the data was copied from external storage medium.

Schran discloses the privacy scanning algorithm to remove unwanted cookie files from the client machine 20. The privacy scanning algorithm determines which cookie files are to be removed (scrubbed) from the client machine 20 by analyzing the privacy protection criteria residing within the local copy of the watch list 14, the trustlist 16 and the blacklist 18. As depicted in the table shown in Figure 5, if a cookie file is listed on the watch list, but not on the trustlist, the cookie file will be scrubbed or blocked. Any time that a cookie file appears on the blacklist, the cookie file will be scrubbed or blocked regardless of whether or not it appears on the watch list. The Privacy Scanning Algorithm may be carried out in a periodic mode wherein the algorithm is executed at a

regular interval, specified by the user, to detect and remove unwanted cookie files from the client machine ([0033]). See further Figure 6 for example of blacklisted websites. Note that by definition, a website is a collection of web pages, images, video or other digital assets that is hosted on one or more web servers (e.g. a computer).

It would have been obvious to an ordinary person skilled in the art at the time of the invention was made to incorporate the teachings of Schran with the teachings of Yuji for the purpose of allowing a user to screen cookie files to determine which cookie files should be stored in the user's client machine (e.g., computer) based on the professional recommendations of a service provider ([Abstract] of Schran).

Regarding **claim 11**, Yuji further discloses attribution of said data is detected based on applications which request the storage of said data, at said detecting (*A sending set transmits the data of a gestalt which the inverter changed and which can be distributed with a broadcasting mold*, [0018]).

Regarding **claim 12**, Yuji further discloses attribution of said data is detected by extracting data attribution information which said data contains, at said detecting (*The data is passed to the filer section. Out of the passed data, the filer section identifies expiration date information, significance information and classification information*, [0022]).

Regarding **claims 13**, and **15**, Yuji further discloses it is determined that the storage of said data is to be performed, if attribution of said data shows that said data is information relating to broadcast contents or said data is broadcast content data, at said

determining (*When it is judged that earthquake information, a heavy rain warning, etc. are important for a user as for the classification information which shows the classification of the contents whose information the and it will change into the data of a gestalt which can be distributed*, [0018]. *Since the information which can judge when informational important point or needlessness data are received, hence, does not record unnecessary information*, [0029]).

Regarding **claim 14**, Yuji further discloses it is determined that the storage of said data is to be performed, if attribution of said data shows that said data is now-on-air information including title information of broadcast contents, at said determining (*Classification information of the important information, i.e., earthquake information, a heavy rain warning etc. may be added with the category information which subdivided an informational classification further*, [0018]. *It is inherent that classification and/or category information contains title of the important news / information*).

Regarding **claim 19**, Yuji clearly shows and discloses a computer readable medium including computer executable instructions, wherein the instructions, when executed by a processor (*Figure 1*), cause the processor to perform a method comprising:

detecting step of detecting attribution of storing-target data (*The data is passed to the filer section. Out of the passed data, the filer section identifies expiration date information, significance information and classification information*, [0022]);

determining whether or not the storage of said data is to be performed based on the attribution of said data detected by said detecting (*When having passed over the expiration date, (Y) cancels received data (it does not record) and is completed*, [0022]);

deleting data having higher deletion-target priority than others from among a plurality of stored data, if said determination step determines that the storage of said data is to be performed and a storage medium for storing said data runs out of space, said deletion-target priority being determined based on attribution of said plurality of stored data (*The record control section records the information received from the filter section on a recording device. Here, when the capacity of a recording device is full, the data considered to be the most unnecessary are eliminated in order, judging from significance, classification, information, an expiration date … Moreover, the record control section eliminates automatically the information which has passed over the expiration date in the recorded information*, [0019]), and if attribution of said data shows that said data is content copied from an external storage medium, it is determined that said deletion-target priority of said data is high to delete said data; and

storing said storing-target data in said storage medium after said data deletion step deletes data having higher said deletion-target priority (*When the capacity of a recording device is full, the data considered to be the most unnecessary are eliminated in order, judging from significance, classification information, an expiration date, etc., and the information received newly is recorded*, [0019]).

Yuji does not teach the deletable data attribute is based on whether or not the data was copied from external storage medium.

Schran discloses the privacy scanning algorithm to remove unwanted cookie files from the client machine 20. The privacy scanning algorithm determines which cookie files are to be removed (scrubbed) from the client machine 20 by analyzing the privacy protection criteria residing within the local copy of the watch list 14, the trustlist 16 and the blacklist 18. As depicted in the table shown in Figure 5, if a cookie file is listed on the watch list, but not on the trustlist, the cookie file will be scrubbed or blocked. Any time that a cookie file appears on the blacklist, the cookie file will be scrubbed or blocked regardless of whether or not it appears on the watch list. The Privacy Scanning Algorithm may be carried out in a periodic mode wherein the algorithm is executed at a regular interval, specified by the user, to detect and remove unwanted cookie files from the client machine ([0033]). See further Figure 6 for example of blacklisted websites. Note that by definition, a website is a collection of web pages, images, video or other digital assets that is hosted on one or more web servers (e.g. a computer).

It would have been obvious to an ordinary person skilled in the art at the time of the invention was made to incorporate the teachings of Schran with the teachings of Yuji for the purpose of allowing a user to screen cookie files to determine which cookie files should be stored in the user's client machine (e.g., computer) based on the professional recommendations of a service provider ([Abstract] of Schran).

Regarding **claim 20**, Yuji further discloses attribution of said data is detected based on applications which request the storage of said data, at said detecting (*A*

sending set transmits the data of a gestalt which the inverter changed and which can be distributed with a broadcasting mold, [0018]).

Regarding **claim 21**, Yuji further discloses attribution of said data is detected by extracting data attribution information which said data contains, at said detecting (*The data is passed to the filer section. Out of the passed data, the filer section identifies expiration date information, significance information and classification information*, [0022]).

Regarding **claim 22**, Yuji further discloses a data storage control program, wherein it is determined that the storage of said data is to be performed, if attribution of said data shows that said data is related information relating to broadcast contents, at said determining (*When it is judged that earthquake information, a heavy rain warning, etc. are important for a user as for the classification information which shows the classification of the contents whose information the and it will change into the data of a gestalt which can be distributed*, [0018]. *Since the information which can judge when informational important point or needlessness data are received, hence, does not record unnecessary information*, [0029]).

Regarding **claim 24**, Yuji clearly shows and discloses a data storage control apparatus ([0018]-[0022]), comprising:

data attribution detection unit configured to detect attribution of storing-target data (*The data is passed to the filer section. Out of the passed data, the filer section*

identifies expiration date information, significance information and classification information, [0022]);

determination means for determining whether or not the storage of said data is to be performed based on the attribution of said data detected by said data attribution detection means (*When having passed over the expiration date, (Y) cancels received data (it does not record) and is completed*, [0022]);

data deletion unit configured to delete data having higher deletion-target priority than others from among a plurality of stored data, if said determination means determines that the storage of said data is to be performed and a storage medium for storing said data runs out of space, said deletion-target priority being determined based on attribution of said plurality of stored data (*The record control section records the information received from the filter section on a recording device. Here, when the capacity of a recording device is full, the data considered to be the most unnecessary are eliminated in order, judging from significance, classification, information, an expiration date … Moreover, the record control section eliminates automatically the information which has passed over the expiration date in the recorded information*, [0019]), and said data deletion unit is configured to determine that said deletion-target priority of said data is high to delete said data if attribution of said data shows that said data is content copied from an external storage medium;

data storage unit configured to store said storing-target data in said storage medium after said data deletion means deletes data having higher said deletion-target priority (*When the capacity of a recording device is full, the data considered to be the*

most unnecessary are eliminated in order, judging from significance, classification information, an expiration date, etc., and the information received newly is recorded, [0019]).

Yuji does not teach the deletable data attribute is based on whether or not the data was copied from external storage medium.

Schran discloses the privacy scanning algorithm to remove unwanted cookie files from the client machine 20. The privacy scanning algorithm determines which cookie files are to be removed (scrubbed) from the client machine 20 by analyzing the privacy protection criteria residing within the local copy of the watch list 14, the trustlist 16 and the blacklist 18. As depicted in the table shown in Figure 5, if a cookie file is listed on the watch list, but not on the trustlist, the cookie file will be scrubbed or blocked. Any time that a cookie file appears on the blacklist, the cookie file will be scrubbed or blocked regardless of whether or not it appears on the watch list. The Privacy Scanning Algorithm may be carried out in a periodic mode wherein the algorithm is executed at a regular interval, specified by the user, to detect and remove unwanted cookie files from the client machine ([0033]). See further Figure 6 for example of blacklisted websites. Note that by definition, a website is a collection of web pages, images, video or other digital assets that is hosted on one or more web servers (e.g. a computer).

It would have been obvious to an ordinary person skilled in the art at the time of the invention was made to incorporate the teachings of Schran with the teachings of Yuji for the purpose of allowing a user to screen cookie files to determine which cookie

files should be stored in the user's client machine (e.g., computer) based on the professional recommendations of a service provider ([Abstract] of Schran).

Regarding **claim 25**, Yuji further discloses said data attribution detection unit is configured to detect attribution of said data based on applications which request the storage of said data (*A sending set transmits the data of a gestalt which the inverter changed and which can be distributed with a broadcasting mold*, [0018]).

Regarding **claim 26**, Yuji further discloses said data attribution detection unit is configured to extract data attribution information which said data contains to detect attribution of said data (*The data is passed to the filer section. Out of the passed data, the filer section identifies expiration date information, significance information and classification information*, [0022]).

Regarding **claims 27**, and **29**, Yuji further discloses the determination unit is configured to determine the storage of said data is to be performed, if attribution of said data shows that said data is information relating to broadcast contents or said data is broadcast content data (*When it is judged that earthquake information, a heavy rain warning, etc. are important for a user as for the classification information which shows the classification of the contents whose information the and it will change into the data of a gestalt which can be distributed*, [0018]. *Since the information which can judge when informational important point or needlessness data are received, hence, does not record unnecessary information*, [0029]).

Regarding **claim 28**, Yuji further discloses the determination unit is configured to determine the storage of said data is to be performed, if attribution of said data shows that said data is now-on-air information including title information of broadcast contents (*Classification information of the important information, i.e., earthquake information, a heavy rain warning etc. may be added with the category information which subdivided an informational classification further*, [0018]. *It is inherent that classification and/or category information contains title of the important news / information*).

13. **Claims 7-8**, **16-17**, **23**, **30-31**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Yuji (*Pub. No. JP 2003-173278, published on June 20, 2003*) in view of Schran et al. (*Pub. No. US 2002/0143770, filed on March 28, 2001; hereinafter Schran*), and further in view of Wright, JR. (*Pub. No. US 2004/0122873, filed on December 20, 2002*; *hereinafter Wright*).

Regarding **claims 7-8**, and **30**, Yuji, as modified by Schran, does not explicitly disclose if attribution of said data shows that said data is information relating to storage media / compact discs, said data deletion means determines that said deletion-target priority of said data is high to delete said data.

Wright discloses a file can have an attribute indicating the file is deletable associated with it. The attribute is indicative that the file is deletable to software, such as operating system software; or file system software or to a user, such as a system administrator, that the file is deletable. Wright further discloses that a file can include any collection of data that is treated by a system accessing the data as a unit capable of being input and output. Therefore, a file can include any directory entry, including a

single file name, a group of file names, a sub-directory, a directory or other set or subset of data units ([0025]).

It would have been obvious to a person with ordinary skills in the art at the time of the invention to incorporate the teachings of Wright with the teachings of Yuji, as modified by Schran, for the purpose of facilitating management of free file space by deleting files using their corresponding delete priorities ([0006] of Wright).

Regarding **claims 16-17**, **23**, and **31**, Wright further discloses if attribution of said data shows that said data is information relating / corresponding to storage media/compact discs, it is determined that said deletion-target priority of said data is high to delete said data (*a file can have an attribute indicating the file is deletable associated with it. The attribute is indicative that the file is deletable to software, such as operating system software; or file system software or to a user, such as a system administrator, that the file is deletable. A file can include any collection of data that is treated by a system accessing the data as a unit capable of being input and output. Therefore, a file can include any directory entry, including a single file name, a group of file names, a sub-directory, a directory or other set or subset of data units*, [0025]).

Conclusion

14. These following prior arts made of record and not relied upon are considered pertinent to Applicant's disclosure:

Furuya (Pat. No. US 6,628,936) teaches communication terminal device.

Borland (Pat. No. US 6,320,943) teaches electronic directory system and method.

Sato et al. (Pat. No. US 7,103,369) teaches system and method for obtaining content relating to a predicted location of a terminal apparatus.

The Examiner requests, in response to this Office action, support(s) must be shown for language added to any original claims on amendment and any new claims. That is, indicate support for newly added claim language by specifically pointing to page(s) and line no(s) in the specification and/or drawing figure(s). This will assist the Examiner in prosecuting the application.

When responding to this office action, Applicant is advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

Contact Information

15. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Son T. Hoang whose telephone number is (571) 270-1752. The Examiner can normally be reached on Monday - Friday (7:30 AM – 5:00 PM).

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Christian Chace can be reached on (571) 272-4190. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Son T Hoang/
Examiner, Art Unit 2165
August 11, 2008

/S. P./
Primary Examiner, Art Unit 2164

/Christian P. Chace/
Supervisory Patent Examiner, Art Unit 2165